Office of the Information
and Privacy Commissioner
of Alberta

OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER
For
British Columbia

Questions and Answers regarding the application of PIPEDA, Alberta and British Columbia's Personal Information Protection Acts (PIPAs)

NOTE: This was written assuming that the Federal Cabinet will declare B.C. and Alberta's Personal Information Protection Acts to be substantially similar to PIPEDA.

Questions & Answers

NOTICE: This document has been prepared in consultation among the offices of the privacy commissioners of Alberta, British Columbia, and Canada. Quebec has a private sector privacy law that has been declared substantially similar to PIPEDA, but that legislation is not discussed in this document.

Introduction:

This document is intended to answer questions organizations and individuals may have about how private sector privacy laws work together. Federal law, the *Personal Information Protection and Electronic Documents Act* (PIPEDA), sets national standards for privacy practices in the private sector. Alberta and British Columbia have both passed similar laws, known in each province as the *Personal Information Protection Act* (PIPA). The provinces have been given assurances that their laws will be soon declared as substantially similar to PIPEDA. This will not mean however, that PIPEDA has no relevance in British Columbia and Alberta, as questions and answers below will indicate.

This document is for general guidance only and is not advice on any specific matter. Always consider getting qualified advice on the facts of any matter before proceeding.

Overview:

1. **What do the federal, Alberta and British Columbia private sector privacy laws have in common?**

The federal *Personal Information Protection and Electronic Documents Act* (PIPEDA), the Alberta *Personal Information Protection Act* (PIPA) and the British Columbia *Personal Information Protection Act* (PIPA) all share the same explicitly stated purpose:

To govern the collection, use and disclosure of personal information by private sector organizations in a manner that recognizes both the right of the individual to have his or her personal information protected and the need of organizations to collect, use and disclose personal information for purposes that a reasonable person would consider appropriate.

2. What are key points about PIPEDA, PIPA Alberta and PIPA BC?

- PIPEDA applies to federal works, undertakings or businesses (FWUBs).
- PIPEDA applies to the collection, use and disclosure of personal information in the course of a commercial activity and across borders. PIPEDA also applies within provinces without substantially similar private sector privacy legislation.
- PIPEDA applies to employee information only in connection with a FWUB.
- The provincial PIPAs apply to provincially regulated private sector organizations.
- Employee information held by provincially-regulated organizations in Alberta and B.C. is covered by the provincial PIPAs.

3. Do the other Canadian provinces have private sector privacy laws?

Quebec has a private sector privacy law that has been deemed substantially similar to PIPEDA. At this point, no similar general private sector laws are before a provincial legislature.

4. What are the common key principles among the private sector privacy laws?

An important principle in all three laws is that an organization may collect, use or disclose personal information only for a purpose that a reasonable person would consider appropriate in the circumstances. All of these laws apply to "organizations" and incorporate the following principles:

- Organizations are accountable for the protection of personal information under their control.
- The purposes for which the personal information is being collected must be identified during or prior to the collection.
- Personal information may only be collected, used or disclosed by an organization with the knowledge and consent of the individual, with limited exceptions as specified in the legislation.
- The collection of personal information is limited to what is necessary for the identified purposes and will be collected by fair and lawful means.
- Personal information must only be used and disclosed for the purposes for which it was collected, except with consent or as required by law. It can be retained only as long as it is necessary to fulfill those purposes.
- Personal information must be as accurate, complete and up-to-date as is necessary.
- Personal information must be protected by adequate safeguards.
- Information about an organization's privacy policies and practices must be readily available to individuals upon request.

- An individual has the right of access to personal information about himself or herself and has the right to seek correction. Both these rights are subject to some exceptions as specified in each statute.

- Organizations must provide the means for an individual to challenge an organization's compliance of the above principles.

Key Definitions:

1. What is personal information?

"Personal information" means information about an identifiable individual which includes any factual or subjective information about that individual, including, for example:

- Name
- Birth date
- Physical description
- Gender
- Address
- Education
- Employment
- Opinions about the individual
- Income
- Medical history
- Religion
- Political affiliations and beliefs
- Visual images such as photographs, and videotape where individuals may be identified

2. What is an "organization"?

An "organization" is defined a little differently in each law. An organization may or may not be incorporated. It may be an individual acting in a business capacity. It may be a non-profit association. Alberta's PIPA specifically includes professional regulatory organizations, whereas in B.C. they are covered by the B.C. *Freedom of Information and Protection of Privacy Act*.

The following are definitions of "organization" in:

PIPEDA [s.2(1)]:

"organization" includes an association, a partnership, a person and a trade union.

PIPA Alberta [s.1(i)]:

"organization" includes
(i) a corporation,
(ii) an unincorporated association,
(iii) a trade union as defined in the Labour Relations Code,
(iv) a partnership as defined in the Partnership Act, and
(v) an individual acting in a commercial capacity,
but does not include an individual acting in a personal or domestic capacity;

PIPA BC (s.1) :

"organization" includes a person, an unincorporated association, a trade union, a trust or a not for profit organization, but does not include

(a) an individual acting in a personal or domestic capacity or acting as an employee,
(b) a public body,
(c) the Provincial Court, the Supreme Court or the Court of Appeal,
(d) the Nisga'a Government, as defined in the Nisga'a Final Agreement, or
(e) a private trust for the benefit of one or more designated individuals who are friends or members of the family of the settler.

3. What is an "individual"?

"Individual" is not defined. However, it means a natural person. An individual does not have to be a Canadian citizen or a resident of a specific province. An individual does not have to be an adult. In some cases a legal guardian or an authorized representative may act on behalf of an individual.[1] Such representatives will be asked to provide evidence of their authority.

4. What is a commercial activity?

"Commercial activity" is defined in PIPEDA. It is also defined in Alberta's PIPA but only as it pertains to certain non-profit organizations. "Commercial activity" is not defined in B.C.'s PIPA because the distinction between commercial and non-profit is not relevant under that law.

Organizations generally thought of as non-profit may have some commercial activities. Commercial activities include, for example, the selling, bartering, or leasing of donor, membership or other fundraising lists. Money does not have to change hands for an activity to be commercial in nature. It is possible that a non-profit organization may, in part of its activities or even a single transaction, engage in a commercial activity.

5. Who oversees compliance with the privacy laws?

Under each privacy law, a Commissioner is designated for overseeing the application of the statute and investigating disputes between individuals and organizations. Each Commissioner heads an organization devoted to oversight of that law (and sometimes other laws as well). Because these officials and their offices have different names, we refer to them in this document generically as a "privacy office". "Privacy office" has no meaning in law.

- For PIPEDA, the privacy office is the Office of the Privacy Commissioner of Canada http://www.privcom.gc.ca/
- In Alberta, the privacy office is the Office of the Information and Privacy Commissioner of Alberta http://www.oipc.ab.ca/
- In British Columbia, the privacy office is the Office of the Information and Privacy Commissioner for British Columbia http://www.oipc.bc.ca/
- In Quebec, the privacy office is The Commission d'accès à l'information du Quebec http://www.cai.gouv.qc.ca/

[1] Who can act for others is outlined in Alberta's PIPA in s. 61(1). In B.C. this information is contained in the PIPA Regulation, ss. 2 to 4. In terms of PIPEDA, this information is contained in Principle 4.3.6 of Schedule 1. Examples common to all include: legal guardians for incapable minors, personal representatives in the administration of a deceased person's estate, and an attorney with relevant power of attorney.

Application of the laws

1. Does PIPEDA apply throughout Canada?

Organizations in the Northwest Territories, Yukon and Nunavut are considered FWUBs and therefore are covered by PIPEDA.

PIPEDA does not apply to provincially-regulated organizations within the province of Quebec. It will not apply to provincially-regulated organizations in Alberta or British Columbia once the privacy laws in those provinces have received substantially similar status from the federal cabinet. However, FWUBs operating in these provinces continue to be subject to PIPEDA. PIPEDA also applies to inter-provincial and international transactions involving personal information in the course of commercial activities.

2. What are some indications that my organization is subject to PIPEDA?

If your organization is a FWUB it would have to comply only with PIPEDA. FWUBs include:

- Banks
- Radio and television stations
- Inter-provincial trucking
- Airports and airlines
- Navigation and shipping by water
- Telecommunication companies such as internet service providers, phone (cellular or land line companies) and cable companies
- Railways, canals, pipelines, ferries, etc. that cross borders

If your organization is not a FWUB but engages in commercial activities that involve inter-provincial or international personal information flows, it would have to comply with PIPEDA ***for these transactions***. For example, an import and export business or credit bureau would have to comply with PIPEDA regarding cross-border personal information collection, use or disclosure.

If your organization is not a FWUB and operates wholly within a province **without a substantially similar private sector privacy law,** it would have to comply with PIPEDA, but only for commercial transactions. Again, B.C., Alberta and Quebec have these laws in place, so PIPEDA applies in the other provinces.

3. How do I know which private sector privacy law applies to my organization?

Firstly, what province do you operate in?

- If your organization is not a FWUB and it operates internally in a province with private sector privacy legislation deemed to be substantially similar (B.C., Alberta, and Quebec), you will have to comply with that province's law
- If your province does not have private sector privacy legislation, PIPEDA is the only statute that might apply. PIPEDA does not apply to employee information in provincially-regulated organizations.
- If you operate in more than one province, you may have to comply with more than one statute, depending on the jurisdiction.

Secondly, look at the definition of "organization" in the statutes you think might apply.

- Does the definition describe your organization?

Thirdly, look at the "application" section of the statute.

- Does the statute apply to you? For example, most of the personal information held by your organization relates to a program subject to FOIP legislation. Personal information that is subject to FOIP is excluded from B.C. and Alberta PIPAs.

4. **Does PIPEDA apply in the same way to all organizations?**

   - If your organization is a FWUB, PIPEDA applies to all commercial personal information flows and to employee personal information
   - If your organization operates in a province not subject to substantially similar provincial legislation and your organization is not a FWUB, PIPEDA applies to all commercial activities; however, it does not apply to employee information in your organization
   - If your organization operates in a province with substantially similar provincial legislation (B.C., Alberta and Quebec) and has to follow that law, PIPEDA only applies to interprovincial and international transactions.

5. **Does Alberta's PIPA apply in the same way to all organizations?**

   Not all Alberta organizations are covered by PIPA in the same way.

   - There is a certain class of "non-profit organizations" in Alberta for which the Alberta PIPA only applies to their commercial activities.
   - There are special provisions for professional regulatory organizations in Alberta to follow an approved privacy code in place of certain sections of PIPA.

   When Alberta organizations subject to PIPA engage in ***trans-border personal information*** flows for commercial reasons, they must follow PIPEDA for those specific transactions.

6. **Does British Columbia's PIPA apply in the same way to all organizations that are subject to it?**

Yes. However, when British Columbia organizations subject to PIPA engage in commercial trans-border personal information flows, they also have to follow PIPEDA for those specific transactions.

Interprovincial and international trans-border data flows

1. **What is a *trans-border data flow*, and how does it affect the application of private sector privacy laws?**

Trans-border personal information flows in a commercial context are covered by PIPEDA due to the federal government's constitutional power over inter-provincial and international trade and commerce.

Examples of trans-border personal information flows include:

- Selling a mailing list from one province to another,
- Using a national credit reporting bureau based in another province to run a credit check on a credit applicant, and
- Sending customer data to a loyalty program in another country.

If your organization collects, uses or discloses personal information such that it flows outside provincial/territorial borders in commercial activities, PIPEDA will apply to that practice. PIPEDA may not apply to *all* of your organization's operations if:

- You operate in a province with a private sector privacy law,
- Your other operations are not commercial, or
- Your organization is not a FWUB and the personal information relates to employees.

2. What if a trans-border personal information flow is unrelated to a commercial activity?

If there is no commercial activity then PIPEDA does not apply.

- *Commercial activity* is defined in PIPEDA

Application of more than one privacy law

1. Is it possible that more than one privacy law could apply to my organization for the same transaction or information practice?

It may be possible that more than one privacy law applies to records created by an organization. This could be the case if you were on contract to another organization that had to follow a different privacy law than your organization ordinarily would, and your organization was obliged contractually to follow the other organization's rules.

> Example: Your organization (in B.C.) provides counseling services to employees of a railway or airline under an employee assistance program. You may be obliged by contract to follow PIPEDA rules regarding the personal information of the company's employees because the company is a FWUB, even though you follow B.C.'s PIPA for the rest of your own operations.

It could also be the case if you are involved in cross-border personal information flows and you operate in a province with a private sector privacy law other than PIPEDA.

2. If a transaction is subject to both a provincial privacy law and PIPEDA, how do I operate to ensure compliance with more than one privacy law at once?

One part of a transaction (e.g. collection) may be subject to a provincial privacy law while another part of the transaction (disclosure) may be subject to PIPEDA. Organizations faced with this kind of scenario may look at the differences between the laws. Is one more stringent or specific in a particular provision? If you follow the more stringent requirement all the time, you will very likely comply with both laws. The federal privacy commissioner and the commissioners in B.C. and Alberta are working together to ensure a harmonized approach to private sector privacy compliance.

Alberta's and British Columbia's PIPAs have "grandfathering clauses" that deem information collected before January 1, 2004 to have been collected with consent. PIPEDA however, may require that organizations obtain consent to use and disclose information collected before PIPEDA came into force. If your organization has to comply with both pieces of legislation, you could ensure that you communicate with your customers to confirm their continued consent for the collection, use and disclosure of that information. You would be going further than required by PIPA, but would not be contravening it.

3. **If personal information is transferred within one legal entity between provinces, and in one location the organization is subject to a provincial privacy law while the in the other location it is subject to PIPEDA, does the fact that personal information crossed borders make the practice subject to federal oversight?**

Example, a customer in Alberta makes a retail purchase at a local branch of a national chain and charges it to her charge account with that retailer. At the point of sale, the retailer asks for the customer's telephone number. During the transaction, a brief electronic communication with the retailer's credit department database in a PIPEDA province takes place, to ensure that the purchase is within the customer's credit limit. The customer objects to the retailer collecting and recording her phone number on the receipt.

In answering this question, the substance of the transaction and the subject of the complaint would be considered. From the customer's perspective, the transaction takes place in the province. The customer is likely not even aware of the trans-border data flow that took place electronically. If the substance of the complaint is about the collection and use of the telephone number then PIPA applies to both the collection and the use. The fact that a trans-border data flow took place is incidental to the complaint.

Contracting

1. **If my organization (that is subject to B.C. PIPA) contracts out the administration of a customers' awards program to a PIPEDA organization *within the same province*, how do we know what law applies to the information transfers to and from the contractor?**

If the contract you have with the awards program administrator specifies that you have control over the customer information, then this practice is subject to the B.C. PIPA. This is true even though the contractor has temporary physical custody of the records; you continue to have informational control. The contracted organization is subject to your privacy rules for the purpose of this account. The awards program administrator is subject to PIPEDA for its own operations and maybe those of other clients

2. **In the above situation, if my organization is in a different province than the contractor, does PIPEDA apply to any personal information exchange?**

If the contracted activity is one normally conducted in-house (e.g. administration of a customer awards program) and the contract makes it very clear that the information is in the control of your organization, then a trans-border data flow may be considered incidental. B.C.'s PIPA would apply to the collection, use and disclosure of personal information

Complaints

1. **Is it possible that more than one privacy office could have jurisdiction in one complaint?**

Yes. However, Commissioners' offices will coordinate their activities to reduce duplication of effort on the part of the complainant and organization. They are working to develop a harmonized approach to dealing with privacy complaints in the private sector.

2. **Does where an individual lives determine which privacy office I bring my complaint to?**

No. The important factors in determining where to complain are described in the question below.

3. **How does an individual know to which privacy office to make a privacy complaint?**

The important factors are:

- Which privacy law does the organization complained about have to comply with? (see above questions under Application of the Legislation), and
- What personal information practice is the individual is concerned about? (E.g. collection, use, disclosure, safeguarding etc.)

Example, an Alberta company has disclosed personal information to a separate organization in Saskatchewan. If an individual wishes to complain about the disclosure of the personal information from the Alberta company, he or she could direct the complaint to the Alberta Privacy Commissioner. If the individual is complaining about the collection in Saskatchewan of their personal information, he/she may wish to direct the complaint to the Privacy Commissioner of Canada. Lastly, if the complaint concerns the use of the personal information in Saskatchewan, it too would be directed to the Privacy Commissioner of Canada.

4. **Which privacy office deals with a complaint when two organizations are involved, and they each follow different privacy laws?**

This situation might occur when one organization discloses personal information to another organization.

In order to determine the privacy office to which you should direct your complaint, the following factors may be considered:

- Which practice do you object to (e.g., collection, use, refusal of access to your personal information, disclosure, safeguarding, etc)?

- If you are concerned about the organization disclosing your information, then the privacy office that oversees the organization doing the disclosure should receive your complaint.

- Is one of the organizations on contract to the other?
  - If so, the primary organization is probably the one responsible for the information practices of the other. The complainant may be best to complain to the Privacy Office with jurisdiction for the contract.

5. What happens to my case if one privacy office starts to look at my case and then determines that their privacy law doesn't apply?

The office that originally looked into your case will return to you all the information you provided to it. Or, with consent, the original privacy office will forward these materials to the appropriate privacy office on your behalf.

The privacy office will also do what it can to assist you make this transition between offices as seamless as possible, subject to the legal authority they have and their legislated confidentiality provisions.